Release Notes

SonicOS

SonicOS Enhanced 5.1.1.0 Release Notes

Contents

Platform Compatibility

The SonicOS Enhanced 5.1.1.0 release is supported on the following SonicWALL Network Security Appliance (NSA) appliance:

- SonicWALL NSA 240

This release supports the following Web browsers:

- Microsoft Internet Explorer 6.0 and higher
- Mozilla Firefox 2.0 and higher
- Netscape 9.0 and higher
- Opera 9.10 and higher for Windows
- Safari 2.0 and higher for MacOS

3G WWAN Card Support

SonicOS Enhanced firmware provides support for many PC cards and wireless service providers as listed below:

GSM Wireless Carriers (with the exception of AT&T Wireless)

- Option GlobeTrotter GT MAX (Model GTmax World)
- Option GlobeTrotter GT MAX 7.2 Ready (Models GX 201/GX202)
- Option GlobeTrotter HSDPA (Model GT 3G+ EMEA)
- Sierra Wireless AirCard 860
- Sierra Wireless AirCard 875
- Sierra Wireless AirCard 880E Express Card
  (requires SonicWALL PC Card to ExpressCard Adapter, part number 01-SSC-2887)
- Sierra Wireless AirCard 880
- Sierra Wireless AirCard 881

CDMA Wireless Carriers (with the exception of Sprint and Verizon)

- Novatel Wireless Merlin 620
- Novatel Wireless Merlin PC720
- Sierra Wireless AirCard 595

AT&T Wireless

- Option GT Max (Model GTmax World)
- Option GT Max 3.6
- Sierra Wireless AirCard 860
- Sierra Wireless AirCard 875
- Sierra Wireless AirCard 881

Sprint

- Novatel Wireless Merlin S620 (Sprint Mobile Broadband Card)
- Novatel Wireless Merlin S720 (Sprint Mobile Broadband Card)
- Sprint Mobile Broadband Card by Sierra Wireless-AirCard 595

Verizon Wireless

- Novatel Wireless Merlin V620
- Sierra Wireless AirCard 595
- Verizon Wireless V740 ExpressCard
  (requires SonicWALL PC Card to ExpressCard Adapter, part number 01-SSC-2887)

Analog Modem

- Zoom Model 3075 56K V.92 PC Card Modem

Known Issues

This section contains a list of known issues in the SonicOS Enhanced 5.1.1.0 release.

Application Firewall

Symptom	Condition / Workaround	Issue
Application Firewall can fail to match a keyword referenced in an SMTP Client Request policy.	Occurs when an email is sent with an inline attachment that contains the keyword, and the keyword is defined in an application object of type File Content.	71952

Networking

Symptom	Condition / Workaround	Issue
Imported preferences files containing Portshield interfaces result in incorrect VLAN settings on the SonicWALL NSA 240.	Occurs when preferences are imported from SonicWALL TZ and PRO appliances running SonicOS Enhanced 3.x and 4.x firmware versions. When the preferences file contains Portshield V1 interfaces, the interfaces are represented as VLANs in the target system running SonicOS Enhanced 5.x firmware.	72152
The spillover value for WAN load balancing is limited to 100 Mbps.	Occurs when attempting to configure a spillover value of more than 100 Mbps for WAN load balancing on gigabit interfaces.	71816
The WAN probe feature does not work correctly for an interface configured as a PPTP client, causing the interface to failover in a load balancing environment.	Occurs when WAN load balancing is enabled and one of the WAN interfaces is configured as a PPTP client. Ping packets sent to the probe target are successfully handled, but the probe results are unavailable for the PPTP WAN interface.	71768
Microsoft Network (MSN) services on the WAN cannot be accessed from the SonicWALL LAN under certain conditions.	Occurs when the SonicWALL WAN port is configured as a PPPoE client, and connects to the MSN server through a PPPoE server.	71298
ARP requests are unexpectedly forwarded to the bridged interface.	Occurs when a secondary subnet is configured on an interface, using a static route and a static ARP entry, and then another interface is configured as a Layer 2 bridge to the first interface. SonicOS correctly provides the static ARP entry in responses to ARP requests for a short time after rebooting the system, but then begins forwarding the ARP requests to the bridged interface.	71127
The OSPF router ID (such as 10.0.0.2) retains its previous value after being changed.	Occurs when the OSPF authentication mode is “simple password”.	66113

VPN

Symptom	Condition / Workaround	Issue
Fragmented packets are sometimes not handled correctly by site-to-site VPN.	Occurs when site-to-site VPN is configured between the WAN interfaces of two SonicWALL appliances, and both of the following are configured: • A VPN NAT policy is configured for access to the LAN side of the destination appliance. • The destination appliance has both IPS and IP Reassembly enabled.	72178
A remote DHCP client can no longer ping a client connected to the central gateway appliance after that appliance reboots.	Occurs when the remote client receives its IP address by using DHCP over VPN. The client is connected to a remote SonicWALL gateway that communicates with the central gateway / DHCP server over a site-to-site VPN tunnel.	71811
Local users on a SonicWALL appliance cannot access the SonicOS user interface on a remote appliance over a VPN tunnel.	Occurs when the local users are connected to an interface in a custom zone (Zone1) on the local appliance, and the firewall access rules for Zone1 to VPN are configured to allow access to all users, or to specific local users or their corresponding local groups.	71250
In a site-to-site VPN tunnel, continuous ping, HTTP, or HTTPS traffic is temporarily disconnected.	Occurs when the Encryption method is set to None during the IPSec (Phase 2) Proposal.	70339

Users

Symptom	Condition / Workaround	Issue
A local user with wireless guest privileges can still access the WAN and cannot be logged out after the login session expires. The User > Guest Status page displays the Session Expiration as N/A.	Occurs when a guest user is connected to the WLAN over a SonicPoint and remains logged in until the maximum session time is reached and the popup window with the Logout button closes.	71620

Resolved Issues

The following issue is resolved in the SonicOS Enhanced 5.1.1.0 release.

Flash File System

Symptom	Condition / Workaround	Issue
New versions of the SonicWALL NSA 240 hardware are no longer compatible with SonicOS Enhanced 5.1.1.x versions of the firmware.	Occurs because the flash memory in the newer units is provided by a different manufacturer since the original flash is no longer available.	72850

Upgrading SonicOS Enhanced Image Procedures

The following procedures are for upgrading an existing SonicOS Enhanced image to a newer version:

Obtaining the Latest SonicOS Enhanced Image Version

To obtain a new SonicOS Enhanced firmware image file for your SonicWALL security appliance:

1. Connect to your mysonicwall.com account at http://www.mysonicwall.com.
2. Copy the new SonicOS Enhanced image file to a directory on your management station.

You can update the SonicOS Enhanced image on a SonicWALL security appliance remotely if the LAN interface or the WAN interface is configured for management access.

Saving a Backup Copy of Your Configuration Preferences

Before beginning the update process, make a system backup of your SonicWALL security appliance configuration settings. The backup feature saves a copy of your current configuration settings on your SonicWALL security appliance, protecting all your existing settings in the event that it becomes necessary to return to a previous configuration state.

In addition to using the backup feature to save your current configuration settings to the SonicWALL security appliance, you can export the configuration preferences file to a directory on your local management station. This file serves as an external backup of the configuration preferences, and can be imported back into the SonicWALL security appliance.

Perform the following steps to save a backup of your configuration settings and export them to a file on your local management station:

1. On the System > Settings page, click **Create Backup**. Your configuration preferences are saved. The System Backup entry is displayed in the Firmware Management table.
2. To export your settings to a local file, click **Export Settings**. A popup window displays the name of the saved file.

Importing Preferences from SonicOS Standard to SonicOS Enhanced 5.1

The SonicOS Standard to Enhanced Settings Converter is designed to convert a source Standard Network Settings file to be compatible with a target SonicOS Enhanced appliance. Due to the more advanced nature of SonicOS Enhanced, its Network Settings file is more complex than the one SonicOS Standard uses. They are not compatible. The Setting Converter creates an entirely new target Enhanced Network Setting file based on the network settings found in the source Standard file. This allows for a rapid upgrade from a Standard deployment to an Enhanced one with no time wasted in re-creating network policies. **Note**: SonicWALL recommends deploying the converted target Network Settings file in a testing environment first and always keeping a backup copy of the original source Network Settings file.

The SonicOS Standard to Enhanced Settings Converter is available at: https://convert.global.sonicwall.com/

If the preferences conversion fails, email your SonicOS Standard configuration file to settings_converter@sonicwall.com with a short description of the problem. In this case, you may also consider manually configuring your SonicWALL NSA 240.

To convert a Standard Network Settings file to an Enhanced one:

1. Login using your MySonicWALL credentials and agree to the security statement.

   The source Standard Network Setting file must be uploaded to MySonicWALL as part of the conversion process. The Setting Conversion tool uses MySonicWALL authentication to secure private network settings. Users should be aware that SonicWALL will retain a copy of their network settings after the conversion process is complete.
2. Upload the source Standard Network Settings file:
   - Click **Browse**.
   - Navigate to and select the source SonicOS Standard Settings file.
   - Click **Upload**.
   - Click the right arrow to proceed.
3. Review the source SonicOS Standard Settings Summary page.

   This page displays useful network settings information contained in the uploaded source Network Settings file. For testing purposes, the LAN IP of the appliance can be changed on this page in order to deploy it in a testing environment.
   - (Optional) Change the LAN IP address of the source appliance to that of a target testing appliance.
   - Click the right arrow to proceed.
4. Select the target SonicWALL appliance for the Enhanced deployment from the available list.

   SonicOS Enhanced is configured differently on various SonicWALL appliances, mostly to support different interface numbers. As such, the converted Enhanced Network Settings file must be customized to the appliance targeted for deployment.
5. Complete the conversion by clicking the right arrow to proceed.
6. Click the download button and save the new target SonicOS Enhanced Network Settings file.

SonicOS Standard to Enhanced Preferences Caveats List

Common Items

A number of features are shared in SonicOS Standard and Enhanced, leading to elements represented similarly between STD and ENH network settings files. Such common elements are translated to the new Enhanced file.

Not Supported Items

The following items from the SonicOS UI and preferences tags are not supported:

- In Network->Intranet, the settings for the network ranges listed here are not supported when the checkbox is set to “Specified address ranges are attached to the WAN link.”

- In the VPN policy creation, there is a checkbox named "Forward packets to remote VPNs". This setting is normally used in a hub and spoke VPN scenario. In ENH, the local and destination networks are explicitly specified. This setting is translated only when there is more than one VPN policy that has the checkbox enabled. This is supported in ENH firmware by adjusting the local networks of each policy to include the remote networks of every other policy.
- When translating access rules, the destination IP addresses are compared to the entries from the One-to-One NAT table. When a matching range is found in that table, the destination network in the translated access rule will contain the public IP address object rather than the private address object.
- For firewalls with the WLAN connections, there is a checkbox and a configuration section in WGS->Settings called "Enable URL Allow List for Unauthenticated Users". In ENH, this has been replaced with address objects and address objects at the moment does not support URLs.
- Certificates are not translated at all as these belong to unique firewalls.
- Upgrade keys are not translated as these are unique to each firewall.

Naming Conventions

The biggest difference in between SonicOS Standard and Enhanced is the way that Enhanced increases network policy granularity through the use of network objects. While initially time consuming to set up, an extensive object library allows a network administrator to define very specific and effective network policies.

As part of the conversion to Enhanced, the Standard policies found in the Standard Network Settings file are broken down into logical network objects and are named in the following way:

VPN Policies

- The destination networks in VPN policies are replaced with address objects. The naming convention for the address objects created are: “policy-name”-local and “policy-name”-remote.
- Access rules are also created depending on the checkboxes per policy.
- STD VPN Policies refer to its local networks using the termination point. There are three choices, a) LAN, b) DMZ and c) LAN and DMZ. In order to support this in ENH, the local networks are pointed to the appropriate subnets object. If the termination point is LAN and DMZ, an address group containing both the LAN and DMZ subnets is created and used as its local network.

Address Objects

- The naming convention for address objects is to use the IP address as its name as well.

Interfaces

- Ungrouped items referring to LAN/WAN/DMZ in STD are set to the correct interface and zone objects in ENH.
- If LAN subnets are supported in ENH, the tool creates the appropriate ARP entry/ies, routing entry/ies and address objects.

Access Rules

- Address Objects referring to the source/destination are created.
- Schedule objects are created if a time constraint is configured in Standard.
- In Standard, certain services can be configured to pass through the firewall from LAN to WAN unimpeded (i.e., the access rules are ignored). A Service Object group is created for these services and an access rule allowing the traffic for these services to flow between LAN/WAN.
- HTTP/HTTPS/Ping/SNMP management are derived from default rules in STD and set in the proper interfaces in ENH.
- The order of the access rules in Standard is not followed when translated to ENH because the access rules from Standard can have multiple equivalents in ENH. Also, the default rules are ensured to remain as the lowest priority.

NAT Policies

- SonicOS Standard One-to-One NAT policies are translated to appropriate NAT policies in SonicOS Enhanced, which may include the creation of address objects when necessary.
  Note that in order to support One-to-One NAT correctly, the address ranges specified in a One-to-One NAT policy requires that we create individual address objects for each IP address in the range.

Services

- Default Service items in STD are translated to equivalent ENH address objects.
- Additional service items are also translated into new service objects.
- Service Object groups were supported in STD by using similar names. An equivalent ENH service object group is created in this case.

DHCP Server

- Dynamic and Static lease settings require creation of its equivalent ENH settings.

IP Helper

- NetBIOS settings in STD are supported by creating appropriate IP Helper policies. This is not supported yet.

Users

- Local users are translated to equivalent ENH users
- Passwords are copied over to ENH and the tool also updates the tag that is used for encryption.
- User properties were supported by checkboxes in STD. This is supported in ENH by adding the user to a group that supports the property (e.g., Limited Admin, Bypass Auth, etc.)

Wireless

- If WLAN restricts certain MAC addresses, MAC address objects are created and added to a group of objects with the name “WLAN ACL MAC Access Denied”.
- If WLAN allows certain MAC addresses, MAC address objects are created and added to a group of objects with the name “WLAN ACL MAC Access Allowed".
- The set of authorized access points also require the creation of MAC address objects and group.
- Guest Profiles are translated to ENH directly.
- Configured items in Wireless guest services are translated to correct users in ENH.

Static Routes

- Static routes are translated by creating address objects for the destination network, the gateway and adding the static route in the routing section for the ENH firmware.

Transparent Mode

- Transparent mode between WAN and DMZ is translated by creating address objects for each of the ranges defined and then creating an address group containing the address objects created. The address group is then used for the DMZ configuration in ENH.
- Transparent mode between WAN and LAN is supported in a similar manner as the WAN/DMZ pairing and the network ranges are created depending on the settings from the Network->Intranet page in Standard.

Upgrading a SonicOS Enhanced Image with Current Preferences

Perform the following steps to upload new firmware to your SonicWALL appliance and use your current configuration settings upon startup:

1. Download the SonicOS Enhanced firmware image file from mysonicwall.com and save it to a location on your local computer.
2. On the System > Settings page, click **Upload New Firmware**.
3. Browse to the location where you saved the SonicOS Enhanced firmware image file, select the file, and click **Upload**.
4. On the System > Settings page, click the **Boot** icon in the row for **Uploaded Firmware**.
5. In the confirmation dialog box, click **OK**. The SonicWALL restarts and then displays the login page.
6. Enter your user name and password. Your new SonicOS Enhanced image version information is listed on the System > Settings page.

Upgrading a SonicOS Enhanced Image with Factory Defaults

Perform the following steps to upload new firmware to your SonicWALL appliance and start it up using the default configuration:

1. Download the SonicOS Enhanced firmware image file from mysonicwall.com and save it to a location on your local computer.
2. On the System > Settings page, click **Create Backup**.
3. Click **Upload New Firmware**.
4. Browse to the location where you saved the SonicOS Enhanced firmware image file, select the file, and click **Upload**.
5. On the System > Settings page, click the **Boot** icon in the row for **Uploaded Firmware with Factory Default Settings**.
6. In the confirmation dialog box, click **OK**. The SonicWALL restarts and then displays the login page.
7. Enter the default user name and password (admin / password) to access the SonicWALL management interface.

Using SafeMode to Upgrade Firmware

If you are unable to connect to the SonicWALL security appliance's management interface, you can restart the SonicWALL security appliance in SafeMode. The SafeMode feature allows you to quickly recover from uncertain configuration states with a simplified management interface that includes the same settings available on the System > Settings page.

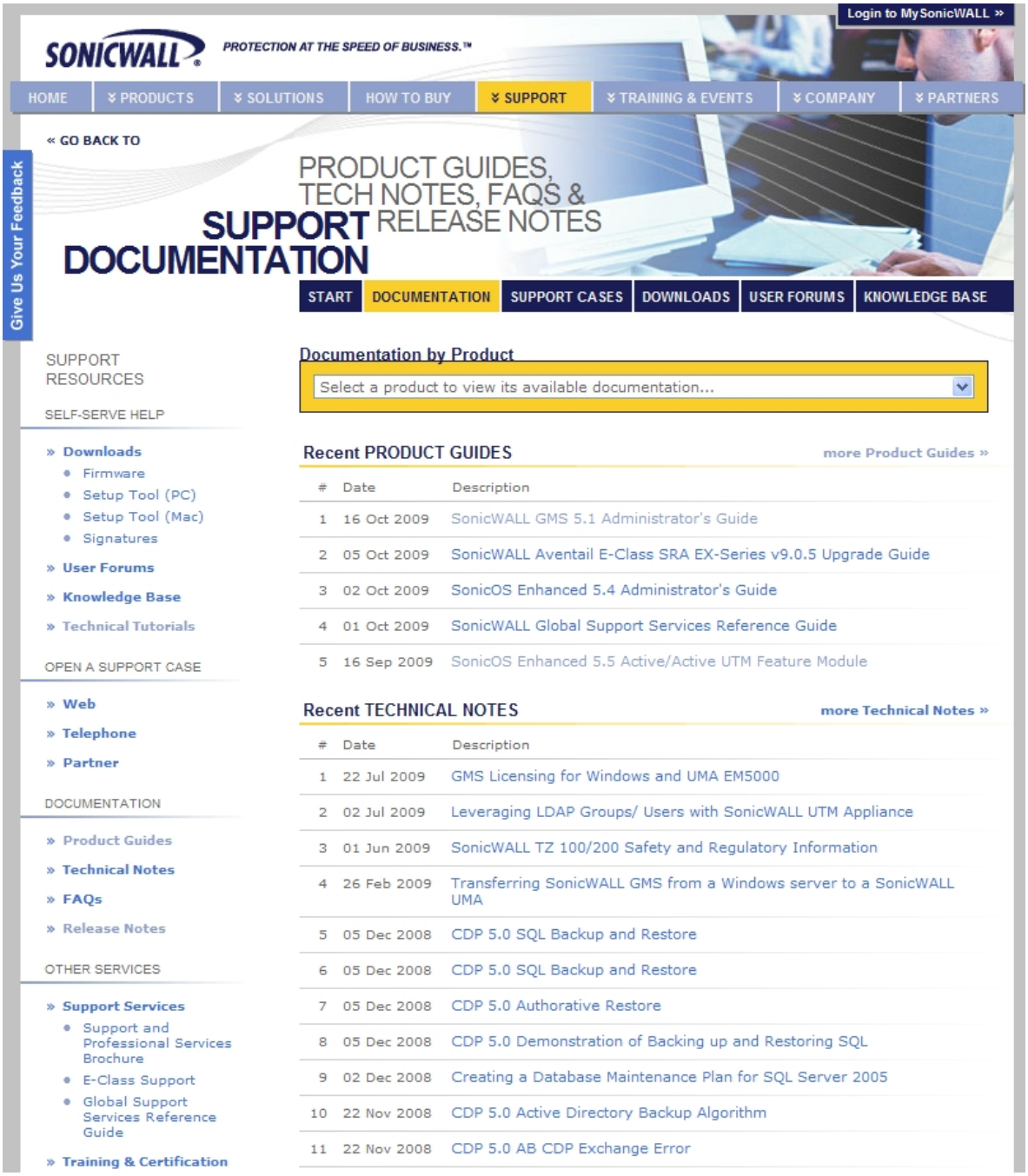
To use SafeMode to upgrade firmware on the SonicWALL security appliance, perform the following steps:

1. Connect your computer to the X0 port on the SonicWALL appliance and configure your IP address with an address on the 192.168.168.0/24 subnet, such as 192.168.168.20.
2. Use a narrow, straight object, like a straightened paper clip or a toothpick, to press and hold the reset button on the security appliance for one second. The reset button is located on the back of the appliance next to the power connector.
   The **Test** light starts blinking when the SonicWALL security appliance has rebooted into SafeMode.
3. Point the Web browser on your computer to **192.168.168.168**. The SafeMode management interface displays.
4. If you have made any configuration changes to the security appliance, select the **Create Backup On Next Boot** checkbox to make a backup copy of your current settings. Your settings will be saved when the appliance restarts.
5. Click **Upload New Firmware**, and then browse to the location where you saved the SonicOS Enhanced firmware image, select the file, and click **Upload**.
6. Select the boot icon in the row for one of the following:
   - **Uploaded Firmware – New!**
     Use this option to restart the appliance with your current configuration settings.
   - **Uploaded Firmware with Factory Defaults – New!**
     Use this option to restart the appliance with default configuration settings.
7. In the confirmation dialog box, click **OK** to proceed.
8. After successfully booting the firmware, the login screen is displayed. If you booted with factory default settings, enter the default user name and password (admin / password) to access the SonicWALL management interface.

Related Technical Documentation

SonicWALL user guides and reference documentation is available at the SonicWALL Technical Documentation Online Library: http://www.sonicwall.com/us/Support.html

For basic and advanced deployment examples, refer to SonicOS Guides and SonicOS TechNotes available on the Web site.



Last updated: 10/19/2009